



9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 105

[USCG-2012-0907]

Port Authority Access to Facility Vulnerability Assessments  
and the Integration of Security Systems

AGENCY: Coast Guard, DHS.

ACTION: Notice and request for comments.

-----

SUMMARY: This notice requests comments from facility owners and operators, State and local law enforcement agencies, port authorities, relevant security industry participants, and all other interested members of the public regarding how to best implement Section 822 of the Coast Guard Authorization Act of 2010. In particular, this notice discusses the Coast Guard's preliminary thoughts on how owners or operators of certain facilities might make their Facility Vulnerability Assessments available to certain law enforcement agencies and port authorities, and integrate their facility security systems with compatible systems operated or maintained by certain law enforcement agencies and the Coast Guard.

DATES: Comments and related material must either be submitted to our online docket via <http://www.regulations.gov> on or before [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] or reach the Docket Management Facility by that date.

ADDRESSES: You may submit comments identified by docket number USCG-2012-0907 using any one of the following methods:

(1) Federal eRulemaking Portal:

<http://www.regulations.gov>.

(2) Fax: 202-493-2251.

(3) Mail: Docket Management Facility (M-30), U.S. Department of Transportation, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590-0001.

(4) Hand delivery: Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

To avoid duplication, please use only one of these four methods. See the "Public Participation and Request for Comments" portion of the SUPPLEMENTARY INFORMATION section below for instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice, call or e-mail Lieutenant Commander José L.

Ramírez, Office of Port and Facility Compliance, Cargo and Facility Division (CG-FAC-2), U.S. Coast Guard Headquarters; telephone 202-372-1150, e-mail Jose.L.Ramirez@uscg.mil. If you have questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202-366-9826.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

We encourage you to submit comments and related material. All comments received will be posted, without change, to <http://www.regulations.gov> and will include any personal information you have provided.

Submitting comments: If you submit a comment, please include the docket number for this notice (USCG-2012-0907) and provide a reason for each suggestion or recommendation. You may submit your comments and material online, or by fax, mail or hand delivery, but please use only one of these means. We recommend that you include your name and a mailing address, an e-mail address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

To submit your comment online, go to <http://www.regulations.gov> and use "USCG-2012-0907" as your search term. Locate this notice in the search results and

click the "Comment Now" box to submit your comment. If you submit your comments by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period.

Viewing the comments: To view the comments, go to <http://www.regulations.gov> and use "USCG-2012-0907" as your search term. Filter the results by checking the box for "Public Submissions" on the left side of the page. If you do not have access to the Internet, you may view the docket online by visiting the Docket Management Facility in Room W12-140 on the ground floor of the Department of Transportation West Building, 1200 New Jersey Avenue SE, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. We have an agreement with the Department of Transportation to use the Docket Management Facility.

Privacy Act: Anyone can search the electronic form of comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor

union, etc.). You may review a Privacy Act, system of records notice regarding our public dockets in the January 17, 2008, issue of the Federal Register (73 FR 3316).

Public meeting: After considering public comments, we may hold one or more future public meetings to provide another forum for public comment. We will announce the time and place of any future public meetings by a later notice in the Federal Register.

#### BACKGROUND AND PURPOSE

Section 822 of the Coast Guard Authorization Act of 2010 (Pub. L. 111-281, 124 Stat. 2905) (CGAA 2010) amended 46 U.S.C. 70102 by imposing the following mandates: (1) the owner or operator of a facility must make a current copy of the Facility Vulnerability Assessment (FVA) available to the "port authority with jurisdiction of the facility" and "State or local law enforcement agencies;" and (2) the owner or operator of a facility must "integrate, to the maximum extent practical," the facility's security systems "with compatible systems operated or maintained by State, law enforcement agencies, and the Coast Guard." Section 822 is intended to increase industry stakeholder and government agency (local, State, and Federal) collaboration efforts to identify, prevent, mitigate, and respond to Transportation Security Incidents (TSIs) and other disasters. If the Coast

Guard undertakes a future rulemaking to implement Section 822, it would apply to facilities regulated by the Coast Guard under the Maritime Security Transportation Act of 2002 (MTSA).

Existing Coast Guard regulations include a number of provisions that require facility owners and operators to ensure the timely involvement of law enforcement and emergency responders in the event of a TSI or other disaster. Each Facility Security Assessment (FSA) must contain provisions for contingency planning, emergency preparedness and response, and communications capabilities (33 CFR 105.305). Facility Security Officers (FSOs) are required to notify law enforcement personnel and other emergency responders, as soon as possible, to permit their timely response to any TSI (33 CFR 105.205(c)(16)). Each facility access point must provide a primary and backup means of contacting police, security control, or an emergency operations center by telephone, cellular phone, portable radio, or other equivalent means (33 CFR 105.235(c) and (d)). State and local emergency responders are not required to obtain or possess a Transportation Worker Identification Credential (TWIC) in order to gain unescorted access to secure areas of a facility during an emergency situation (33 CFR 101.514(d)).

While the Coast Guard believes that in most instances, the measures detailed above are adequate to ensure the timely involvement of State and local law enforcement and emergency responders, additional regulations may be necessary to close potential gaps that might hinder an appropriate emergency response to a TSI or other disaster.

#### Preliminary Alternatives Considered

We have considered a number of possible ways to implement the requirements in Section 822. We describe these approaches below to inform the public of our preliminary thoughts on implementing Section 822 and to solicit public comments to gain a better understanding of the issues that concern affected parties, as well as current industry practices on facility interactions with port authorities, State and local law enforcement agencies, and the Coast Guard. We are also interested in any information and data about the costs associated with these approaches as well as any potential benefit. These comments may assist us in formulating policy as we consider a future rulemaking to implement Section 822.

#### FVA Sharing Alternatives:

- Require each MTSA-regulated facility owner or operator to make a copy of the current FVA available to the cognizant Coast Guard Captain of the Port, port

authority, and State and local law enforcement agencies, upon request. The owner or operator would share the FVA via electronically secured transfer. Do facilities store FVAs electronically?

Are you able to save them as an encrypted or password-protected file?

- Require each MTSA-regulated facility owner or operator to proactively provide a copy of the current FVA to the port authority and State and local law enforcement agencies at a prescribed time interval (as opposed to making copies of FVAs available to the port authorities and law enforcement upon request). The owner or operator would share the FVA via electronically secured transfer.

Are you able to encrypt or password-protect the FVA electronic copy and/or deliver it on a password-protected CD, flash drive, or other storage medium?

- Require each MTSA-regulated facility owner or operator to share the current FVA with the port authority and State and local law enforcement agencies annually at the annual exercise required under 33 CFR 105.220 or at a newly required annual FVA sharing meeting.
- Require each MTSA-regulated facility owner or operator to share the current FVA with the port authority and



State and local law enforcement agencies during the regularly scheduled 5-year resubmission process of the Facility Security Plan (FSP).

- In addition to the requirement to share the current FVA, require each MTSA-regulated facility owner or operator to make the Security Measures Summary (CG-6025) available to the relevant government authorities and law enforcement agencies for review at the end of the required annual exercise or equivalent (33 CFR 105.220).
- In addition to the requirement to share the current FVA, require each MTSA-regulated facility owner or operator to update the FSP to incorporate FVA-sharing measures.

Security System Integration Alternatives:

- Require each MTSA-regulated facility owner or operator to have and demonstrate via annual exercises the ability to provide manual alerts regarding a TSI to appropriate State and local law enforcement agencies and the Coast Guard.

Is 15 minutes a reasonable estimate of the additional time needed to comply with this requirement?

- Require each MTSA-regulated facility owner or operator to have and demonstrate via annual exercises the ability to provide automated alerts regarding a TSI to appropriate State and local law enforcement agencies and the Coast Guard.

Is 15 minutes a reasonable estimate of the additional time needed to comply with this requirement?

- Require each MTSA-regulated facility owner or operator to make security data feeds regarding a TSI (e.g., alerts, video feeds, alarms, etc.) available to appropriate State and local law enforcement agencies and the Coast Guard.

Do appropriate levels of technology exist at both the facility and receiving government agency to comply with this requirement, which would consist of sharing telecommunications information such as Internet addresses, phone numbers, passwords, and encryption codes?

- Require each MTSA-regulated facility owner or operator to incorporate a technological solution that integrates their electronic surveillance and communications systems with compatible systems operated or maintained by the appropriate State and

local law enforcement agencies and the Coast Guard.

There is a range of possible methods for integrating security systems, including Internet connectivity, dedicated telephone lines, and other forms of security system integration.

#### Information Requested

1. We request comments on the feasibility, costs, and benefits of each of the preliminary alternatives described above. Please be as specific as possible. For estimates of costs a break-out by specific cost element would be preferable to a lump sum. For example, provide separate estimates for the equipment, number of hours and type of worker needed to install the equipment (i.e. master electrician, labor, supervisor), number of hours and type of employee (i.e., trainer, mid-level manager) to prepare and execute training, and on-going maintenance costs. Cost estimates can be provided as ranges.

2. We request comments as to whether there are any data, literature, or studies that demonstrate the feasibility, costs, and benefits of each of the preliminary alternatives described above.

3. We request comments from MTSA-regulated facility owners and operators regarding current industry practices with respect to security system integration between the facility

and State and local law enforcement agencies, the Coast Guard and, emergency responders.

4. We request comments as to whether the requirement to integrate facility security systems with those of State and local law enforcement agencies, the Coast Guard, and emergency responders should be limited to only those MTSA-regulated facilities that are identified in risk-based and other applicable types of analyses. If so, please identify the characteristics of those facilities.

5. Aside from the preliminary alternatives described above, please provide any other alternatives on preferred ways to implement the requirements in Section 822. For any such alternatives suggested, please include information and data as to the feasibility, costs, and benefits.

6. We request any additional comments from interested parties on the subject matter of this notice.

This notice is issued under authority of 5 U.S.C. 552(a), 46 U.S.C. §§ 70102(c) and 70124.

Dated: **January 25, 2013**

P. F. Thomas  
Director, Inspections and Compliance  
U.S. Coast Guard

[FR Doc. 2013-02209 Filed 01/31/2013 at 8:45 am; Publication  
Date: 02/01/2013]